PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-152837

(43)Date of publication of application : 16.06.1995

(51)Int.Cl. G06F 17/60
G06K 19/07

(21)Application number : 06-244919

(22)Date of filing : 14.09.1994

(71)Applicant : AT & T CORP

(72)Inventor : MANDELBAUM RICHARD
SHERMAN STEPHEN A
WETHERINGTON DIANE R

(30)Priority

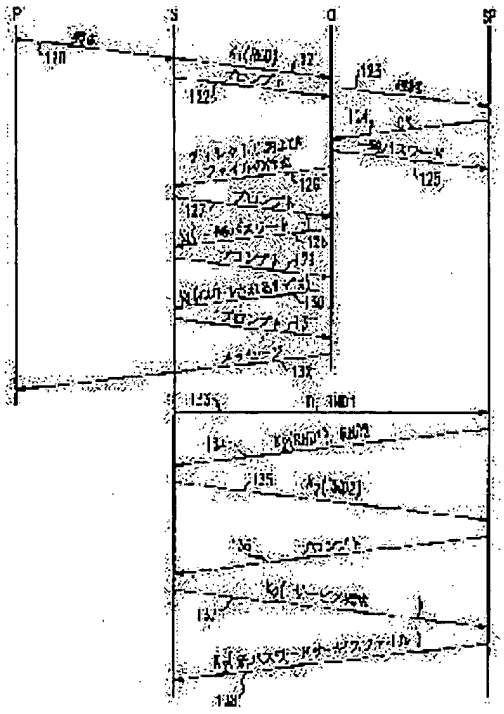
Priority number : 93 122631 Priority date : 17.09.1993 Priority country : US

(54) SMART CARD

(57)Abstract:

PURPOSE: To provide a smart card to which the services of a plurality of service providers are mounted such as overcoming the problem of security and being remotely issued.

CONSTITUTION: The smart card is provided with a memory and a processor relating to an issuing person, an owner and the service provider and is further provided with an operating system provided with a tree-like file structure starting from a file provided with characteristics controlled only by the issuing person and a plurality of executable files respectively provided with the characteristics controlled only by the issuing person for forming a part of the tree-like file structure. The operating system is further provided with password files for respective interested parties accessible only to the interested party to be accessed by the interested party before the interested party becomes accessible to the executable file corresponding to the respective interested parties of the issuing person, the owner and the



service provider.

LEGAL STATUS

[Date of request for examination]	14.04.1997
[Date of sending the examiner's decision of rejection]	06.05.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] In the multiplex application smart card which has the memory and the processor about a publisher/owner, a carrier, and a service provider The operating system which has the tree-like file structure which begins from the file which has the property controlled only by said publisher/owner, Two or more executable files which can be performed for the purpose of forming said a part of tree-like file structure, having the property controlled only by said publisher/owner, respectively, and acting on the permission data in said memory if referred to, The password file accessed by said publisher/owner before it is accessible only to said publisher/owner and said publisher/owner become accessible at said executable file, The password file accessed by said carrier before it is accessible only to said carrier and said carrier becomes accessible at said executable file, The multiplex application smart card characterized by consisting of a password file accessed by said service provider before it is accessible only to said service provider and said service provider becomes accessible at said executable file.
[Claim 2] In the smart card which suits so that it may communicate with a person concerned, and has a processor It is arranged for every user entity in two or more logic zones for informational storing and acquisition. At least two of the logic zones The memory which has a subzone containing the memory segment containing access-control data, Only when said person concerned sends the information related to the access-control data contained in the predetermined logic zone of said logic zones to a smart card The smart card characterized by consisting of a control means which enables said persons concerned also including the subzone to access the predetermined logic zone.
[Claim 3] The operating system which has the tree-like file structure which begins from the directory file which has the attribute controlled only by the 1st person concerned, Two or more executable files which can be performed for the purpose of acting on the permission data in memory if it has the attribute which forms a part of the tree-like file structure, and is controlled only by said 1st person concerned, respectively and is referred to, As opposed to the smart card which consists of a password file accessible only when said 1st person concerned can access said executable file and which is published by said 1st person concerned In the approach of installing the function in which the 2nd person concerned provides the carrier of the smart card with service The step to which said carrier supports establishing the communication link between said smart card and said 1st person concerned, The step which uses the data with which it is contained in said password file, and performs the log in protocol between said smart card and said 1st person concerned, The demand communication link step which communicates the demand which installs a service function on said smart card for said 2nd person concerned to said 1st person concerned, The step to which said 1st person concerned sets the user password file in said smart card so that said a part of tree-like file structure may be formed, The step at which said 1st person concerned inserts data in said user password file, The install approach of a smart card characterized by consisting of a step at which said 1st person concerned changes the file attribute of said user password file so that it may be made accessible only to said 2nd person concerned.
[Claim 4] The approach of claim 3 characterized by having further the step of which said 2nd person concerned is notified about the data stored in said user password file.

[Claim 5] The approach of claim 3 characterized by having further the step which checks that said demand is filled by said 1st person concerned after said demand communication link step to said 2nd person concerned.
[Claim 6] The approach of claim 3 characterized by said communication link using a telecommunication network.
[Claim 7] The correspondence procedure characterized by consisting of the 1st authentication step with which said individual humanity news equipment attests said person concerned by challenge / response sequence, and the 2nd authentication step with which said person concerned attests said individual humanity news equipment by challenge / response sequence in the approach a person concerned communicates with individual humanity news equipment.
[Claim 8] The approach of claim 7 characterized by said 2nd authentication step preceding with said 1st authentication step.
[Claim 9] The approach of claim 7 characterized by the carrier of individual humanity news equipment having further the step attested by individual humanity news equipment by challenge / response sequence.
[Claim 10] The approach of claim 7 characterized by said 1st authentication step being unfinished when said 2nd authentication step is started.
[Claim 11] The step to which, as for said 1st authentication step, said individual humanity news equipment transmits the challenge including ID information and the 1st data string, Said 1st data string is enciphered using the 1st cryptographic key based on ID information transmitted by said individual humanity news equipment. It consists of a step which transmits the 1st data string who enciphered to said individual humanity news equipment. Said 2nd authentication step The step to which said person concerned transmits the challenge including the 2nd data string, The step which enciphers said 2nd data string using the 2nd cryptographic key stored in said individual humanity news equipment in advance, and transmits the 2nd data string who enciphered to said person concerned, The approach of claim 7 characterized by consisting of a step to which said person concerned checks Shinsei of said individual humanity news equipment by said 2nd cryptographic key, and a step with which said person concerned attests said individual humanity news equipment by said 2nd cryptographic key.
[Claim 12] Said 1st data string and said 2nd data string are the approach of claim 11 characterized by consisting of a random sequence.
[Claim 13] Said 1st cryptographic key and said 2nd cryptographic key are the approach of claim 11 characterized by the same thing.

[Translation done.]

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] This invention relates to a smart card.
[0002]
[Description of the Prior Art] It is possible to have great count capacity in small space by progress in microelectronics. It is possible to actually put in the whole computer substantially in a credit card, and the "smart card" is created by this. Being used in order that a smart card may check the right of the card carrier which pulls down from a predetermined account typically and is carried out [for the big throughput of a smart card and memory capability] for the conventional credit card is expected. A smart card offers the guarantee of the high level of the possessor of a smart card being a just carrier. This solves the main problems of the conventional credit card. Furthermore, a smart card becomes a thing more than the "license" for pulling down from an account (an account being transferred). For example, what a smart card "carries for" the credit recognized in advance is made.
[0003] In order to enable a smart card to achieve a convention, a service provider must think it certain that the computer in a smart card cannot use it for an unjust application. In order to satisfy this need, some approaches are already used. A smart card is equipped [1st] with a power-source port and a single information passage port. The computer embedded [2nd] at the smart card operates under control of the operating system which guarantees that the instruction sent to a computer does not perform harmful actuation to the purpose and security guide of a card. That is, only the instruction which reads the permitted data area and which is ordered and changed is possible. Through remote communications, there is no publisher of today's smart card then, and he claims [3rd] using a card within the enclosure of a provider.
[0004]
[Problem(s) to be Solved by the Invention] The memory of a current smart card is sufficient magnitude to hold two or more programs and data of a service provider. That is, the memory of sufficient magnitude for visa, American Express, and a master card to live together is on a single smart card. However, in commercial semantics, the smart card which succeeded in carrying service of two or more service providers is not developed yet. It is thought that this situation is because some security issues are not solved. For example, a problem arises about what kind of authority an owner has to all the files in the memory of who is the owner of a card, and a smart card. It is the problem what authority the owner (this being also a service provider) of a smart card having in the smart card which is not in agreement with the security for which other service providers ask, speaking commercially. This is the problem of trust.
[0005] The 2nd trouble is related with remote issuance. Especially the thing for which it is required for a smart card carrier that service should be installed only by having a card at a provider's place and going is not desirable. Moreover, when one of services on a smart card is canceled, it is not desirable to require the turnover of a smart card, either. Rather, for a commercial success, it is desirable to enable remote issuance, probably it is essential, and clear.

[0006] When the trouble of remote issuance is solved, the 3rd trouble is related with the need of carrying out the reuse of the space in the smart card of a carrier, in case the old service is canceled and new service is installed.
[0007] The 4th trouble is that a provider wants so that it may restrict the commercial collision of a contention service compartment, and that a customer accesses contention service.
[0009]
[Means for Solving the Problem] A service provider or the owner of a smart card does not have authorization in beforehand, and the above-mentioned trouble is solved by the operating system with which a service provider which is different, without accessing the file by which it was created by each existing service provider since it was each existing service provider makes it possible to live together on a smart card.
[0010] The operating system of a smart card resembles UNIX (trademark of UNIX system Laboratories) a little, it has the root directory owned by the publisher/owner of a smart card, and each service provider is a "user" installed by a publisher/owner. The subdirectory of a root directory is given to such each user, and in the subdirectory, a user creates it as a user needs a subdirectory including a file and a file.
[0011] An operating system can be made not to perform such access, when preventing from accessing the file which a user owns from other users to all the users of the smart card containing the publisher / owner of a smart card, and the carrier of a smart card is chosen. This exclusion capacity is owned by the user and other users including the publisher/owner of a smart card are realized by the password file which cannot be changed. As an option, the capacity which eliminates all the files of the given user is given to the publisher/owner of a smart card.
[0012] Moreover, an operating system has means of communications with a digital signature, and full encryption means of communications. This function gives the dependability in remote communications. By remote communications, remote issuance, effective maintenance of the database which pursues all services included in each smart card, and loss of a smart card or re-issuance of the smart card in general failure is attained.
[0013]
[Example] Some smart card operating systems are already known. One example is indicated by U.S. Pat. No. 4,816,653 (artificer: date-of-issue: [besides Anderl (Anderl)] March 28, 1989). The operating system explained below has the operating system and a well-known UNIX operating system, and many similar points. In order to help an understanding of the smart card operating system explained here, the matter of some common knowledge of a UNIX operating system is explained briefly.
[0014] A [UNIX operating system] UNIX operating system consists of a set of a file. Some of the files are called a directory file or a directory, mainly including the information about a related file. Other files are "usually" called file including user data. Moreover, in a UNIX operating system, a user can belong to specified "group (group)" which is "owner (owner)" of a file, or is recognized by the file, or can belong to "other." Each file contains a part for the data division which specifies the file descriptions, such as ownership and information accessing capability about three kinds of users. The owner of a file can change all the file descriptions.
[0015] Structurally, the first file is a root directory file. The user who is the owner of this directory is actually the owner of the whole operating system. This user can create other files to which it is pointed out by the root file. It is considered that the file is possible also for that they are also other "directory" files and being "usually" a file, and is "under" a root directory in tree top structure.
[0016] In many UNIX operating systems, one of the directories under the root is named "etc", and this directory has the file "passwd" in the bottom of it. They are "/etc/passwd" (the file "/" of the beginning of a pathname expresses the root address)., all the addresses, i.e., the pathname, of this file Generally "etc" and the "passwd" file are called the root, and are owned by the system administrator who is also an owner of a root directory. Including the encryption expression of a root password, the "passwd" file is allowed for access of the root to an operating system, only after the root logs in by showing a password. It is enciphered and the password shown is compared with the encryption password stored in the "passwd" file. When a comparison is successful, a user is accepted and access to other files is permitted

to him. That is, "it means that this user had logged in."
[0017] Multiuser ability is realizable, when the root creates a subdirectory under a root directory and assigns other users the ownership of the subdirectory. Next, the root makes it possible to go into a system in the subdirectory file, when the user's password is installed in the "passwd" file and the user presents the password. Although this user has the capacity to change a self password, only by it leading the command offered by the operating system, it is possible. In a system, the password is the enciphered format and exists only in a chisel and the "passwd" file. This architecture is shown in drawing 1 .
[0018] A login process can be summarized as follows. The computer which operates under a UNIX operating system is put into operation by executing the loop formation which scans the input port of a computer. If connection by the user is detected, it will move from control to the program which started the dialogue with the user from the loop formation. The program waits a "login:" message for a response of delivery and a user to a user. Self is displayed and this makes the user identify to an operating system, when a user returns a string "htb." Next, a program must send a demand message "Password:" and a user has to present a password string. A program enciphers the password string and compares it with the encryption password of the user in /etc / "passwd" file who identified. When in agreement, it judges that a user is Shinsei and control is passed to the file (typically, named ".profile") owned by the root. This file sets up various parameters to that user, and is passed to another file (although this is also typically named ".profile", this file exists in the directory owned by that user) owned by the user in control. After the instruction in the user's ".profile" is executed, a computer enters a loop formation and waits for the instruction of the degree from a user.
[0019] The root is the owner of all the files that constitute operating systems including the "passwd" file. Therefore, the root can change the file of arbitration, therefore is a "superuser." Even if it is the file which is not owned by the root, it is important to follow the command of the root. It is because the root has the capacity to also change the file by which the capacity of the root is controlled generally, with the "passwd" file. According to this capacity, the root has the capacity to change a password, therefore the root can always become the owner of a file. Therefore, it is meaningful to give all an owner's capacity directly to the root. If it says briefly, the root has the absolute control and all the information on all the files in a system.
[0020] (An exact password is shown) it can log in -- in addition, read-out of a file, the writing to a file, and the capacity of activation (that is, pass program control to a file) of a file are given to a user. (Nothing can be performed if there is no capacity to pass program control to the specified file.) It is because performing a program is exactly passing control to a file. Since the root can access all the files of a system, the root can read and write in and perform all files.
[0021] An instruction of all system offers of a UNIX operating system is the file which can only be performed, and these files can exist in every directory, as far as the system knows where the file is. As already stated, the root owns such all directories and files. Since the root controls read-out of all those directories and a file and authorization of activation, the root can be restricted by the user (including oneself, in being required) of arbitration by only restricting a file permission (permission) so that the file of arbitration may not be performed. Thereby, the root can create the set in which the file to which activation by a user's specific group was restricted carried out custom-made **. If it puts in another way, the root can create restricted various operating systems which contain commands fewer than all available commands by the system, i.e., "limit shell."
[0022] The absolute capacity which the root has with a [smart card operating system] UNIX operating system is unsuitable to a smart card. Although visa, the master card, and a provider like American Express probably do not permit clearly that it is the root mutually, if there is not sufficient security means clearly, it will also be thought that third persons other than these are not wanted to become the root. This is a part of trouble that a smart card does not store a commercial success which should be received.
[0023] The structure corresponding to the sensitiveness of this service provider is shown in drawing 2 . According to the structure of drawing 2 , the root owns a root directory and a number of arbitration to create of files (a directory file or regular file). For example, as for drawing 2 , there are the ".profile" file

11, the "passwd" file 12, the "log" file 17, the "filex" file 13, the "filey" file 14, and an "ID" file 18 in the bottom of it including the root directory file 10. For the bottom of the root, some subdirectories also exist and it is used as a user's (service provider) "HOME" directory, respectively. For example, drawing 2 contains the directory file 15 of the identifier (carrier of a smart card) of "htb", the directory file 20 named "bankA", and the directory file 25 named "airlineA." Each directory includes the "passwd" file (respectively 16, 21, and 26) and ".profile" file under a corresponding user's HOME directory. This is not indispensable although this arrangement of a password file has some advantages. An important thing is that the ownership of such each password file is assigned to the file and the user corresponding to the directory on [of it]. It is also useful to grant each user the ownership of directories 15, 20, and 25.
[0024] Drawing 2 includes another important directory (and user). It is the "Visitor" directory 30 and this is the entry point of the non-service provider which wants to have a dialog with a smart card.
[0025] The file architecture of drawing 2 is combined with a different operating system from a UNIX operating system. The operating system of the structure of drawing 2 mainly differs from a UNIX operating system with the operating system in that the capacity to change the file which the root does not own is not given to the root. In order to guarantee that this function does not detour by the root, in this operating system, the root does not permit changing some files which define an operating system (in a sense, the root does not own those files). One means to realize this result is storing those non-root possession operating system files in a read-only memory (ROM). This ROM at least includes the command / module / file which performs the writing to a file. Especially the writing to a file is restricted to the thing specified by the owner of a file (the owner of a file is the user who created the file at first), and the root is only treated as other users. The command which performs the writing to a file is an operating system command like migration of a file, the copy of a file, preservation of a file, modification of a file attribute (for example, ownership), and modification of a file name. (Since it is peculiar to each smart card) Other matters installed in ROM (still more generally "1-time write-in" memory) are root run WORD and ID information on a smart card (namely, files 12 and 18). ID information can also include [that he is also only the string of arbitration, and] the identifier of a carrier. It is desirable to include the identifier of a carrier to the merchant who probably acquired ** and ID information. Each ID of root run WORD and a smart card can be stored in the file which constitutes a root directory (namely, block 10) in fact. In drawing 2 , these serve as an independent file for explanation.
[0026] In some the examples, it is the capacity for one file write-in capacity to be given to the root, and for this to delete the file of arbitration as a whole (and the file which is the process and the file deleted substantially has pointed out is deleted). A directory file and a regular file are contained in this, and it is applied also to the file which the root does not own in the file which the root owns, either. Such capacity can be given in the example to which the reuse of the room is carried out, when the given service provider does not provide the carrier of a smart card with service any longer.
[0027] Another difference between the operating system of drawing 2 and a standard UNIX operating system is a point including the code key pair by which the former was installed at the file owned by the root (for example, 13) that this key pair is peculiar to each smart card. the private key f and smart card which are secretly held by the smart card hold this pair secretly -- as -- the open key g which are not careful of is included. Of course, although both keys are known from the beginning at the owner/publisher of the smart card which is also the root user (namely, superuser) of a smart card, the root does not need to hold a private key (and destroying the information probably will be chosen). This key pair can also be included in the file which defines "an eclipse with baking", or a root directory as suitable memory like the memory containing a root password. Open key encryption is further explained to a detail later.
[0028] It is the material-difference point of a UNIX operating system and the operating system of drawing 2 to be stored in the file the password of a user's directory is owned by whose user of the. That any persons other than the owner of the file cannot read these passwords makes it possible to store in the format which does not encipher the password. It becomes impossible for the root to become the owner of the file (a regular file or directory file) of arbitration by this configuration with the limit to writing therefore, and it becomes impossible for the root to bypass the authorization set up by the owner of a

file. With this material-difference point, a certain user's file becomes completely opaque to the root and other users. Thus, the configuration of drawing 2 conquers the "reliance problem" between the provider of service, and the publisher/owner of a smart card.
[0029] The following problem which should carry out [dealings security] solution is the dealings security of a smart card. This concept includes the means used by the operating system of a smart card, and those who have agreed with the communications protocol, in order to guarantee that unauthorized dealings which have a bad influence on the carrier or service provider of a smart card do not take place. This includes the activity by the root, the carrier, the service provider, the visitor (Visitor) user, or the invader. (Invaders are those who intervene in the communication link session between a smart card and the others, and replace a self message with a true message.)
[0030] One method of opposing an invader constitutes the message containing the time stump of a date and time of day, and is a thing of a message for which the part is enciphered at least. Moreover, when required, a communications protocol is possible also for requiring that a check sequence (these differs for every session) should be exchanged between persons concerned. Moreover, the effective general approach also makes min the flow in Akifumi of delicate information like a password. These techniques are used with the below-mentioned log in and a communications protocol.
[0031] The field of [encryption] encryption is not new. The following explanation is the epitomes of two usable cipher systems only in relation to the smart card of this invention.
[0032] As everyone knows, the "secret share" method for encryption requires that two operators should share the secret function f. A way [to transmit Message m] side enciphers the message with the secret function, and forms encryption message f (m). This encryption message is transmitted and a receiving side decodes the signal received by forming Function f (f (m)). Although Function f is very difficult to discover Message m from f (m) in computational complexity, it is the function (namely, f(f (m)) =m) with which the message of a basis is restored by applying the function twice.
[0033] Although the "secret share" method for encryption is very effective, the weak spot is that there is the need (that is, it shares) of communicating a secret function. When a secret shared [the] is acquired by the wire-tapping person during a rare communication link session when the function is transmitted, it becomes already secret less.
[0034] open key encryption -- each person concerned -- a key -- an opposite -- either f or the g are held. Although one person concerned holds one key (f) secretly and does not communicate it especially, all persons are told about the key (g) of another side. therefore, the key g -- "-- it opens to the public -- having -- " -- Key f is "private." Pair f and g seem to fulfill the following three conditions.
1. g(f (m)) =m.
2. Function f cannot be determined even when g is known.
3. It is unrealizable in computational complexity to determine Message m from f (m).
[0035] Although a open key method solves the problem of the above-mentioned key distribution / management, this approach has one fault. It is slower [encryption and decode of a open key] (much computation time is needed) than a share key method.
[0036] About a smart card, transmission speed has a different significance based on the class of person concerned who is communicating with the smart card. about the publisher / owner, and the service provider of a smart card, a rare thing expects a communication link -- having -- therefore, the processing time -- "-- since it is not maximum important", low speeds are not main faults. However, in the communication link with the other person (namely, merchant who logs in as a visitor user), the rate is important.
[0037] The problem of a rate will be solved by combining a "share secret" method with a open key method, if required. That is, when starting a communication link, temporary "share secret" is communicated between a smart card and a merchant using a open key method. Especially the side that has a open key presents a "share secret", and communicates it to the side which has a private key. Then, all messages are enciphered more at a high speed using a "share secret" method.
[0038] Or it is also possible to use an authentication (using share secret) method. By the authentication method, a message is transmitted by Akifumi and a "digital signature" is added (that is, "signed"). A

"digital signature" is the hashing (for example, a certain number addition of the ASCII code of the alphabetic character in a message as law) of the message encoded. Of course, with application it is guaranteed to be that an invader cannot replace true data by fake data, information can be sent by Akifumi (after the validation process which probably used ** and a open key).
[0039] Use of a open key method solves almost all the problems of key management. Although the problem of the initial information on the open key of the person concerned who wants to communicate with a smart card remains in addition, since the smart card itself can offer the information, it is not a problem.
[0040] Since [install of log in [by the root], and service provider/user] encryption guarantees a safe communication link, the publisher/owner of a smart card can trust remote install of service. Of course, a publisher/owner (namely, root) has to log in to a smart card first. The protocol for a log in is shown in drawing 3 . Moreover, the protocol for a service installation process is shown in drawing 4 . Connection of RIMOTO is shown to a possible physical target between the smart cards of this invention at drawing 8 .
[0041] As shown in drawing 3 , a process is started from the possessor (P) of a smart card being attested as a Shinsei smart card (S) carrier. As shown in drawing 3 , a process is started by inputting a possessor's PIN (personal identification number) into a smart card as the prompt from a smart card. It is advantageous to the equipment which may catch PIN to use the throughput of a smart card, in order to attest a possessor at the point that it is not necessary to communicate an PIN string. Even if it is the application with which P and S exist within the enclosure of a merchant, a merchant's equipment can be considered as the equipment of the stand-alone mold which carries out an interface to a smart card at insurance. This equipment can check operating by the cell, having a keyboard and a display, and not having other ports, processors, and memory that can be written in. At the time of actuation, P inserts S in this stand-alone equipment, PIN is inputted by the keyboard, and, as for a smart card, that PIN judges whether it is the right. If right, the display of the equipment will output a message "O.K." When such stand-alone equipment is not available (in the remote ****** case [A communication link like / when using a "dam" card reader at a possessor's home / Or for example,]), PIN shown should be processed within the smart card and it is enciphered by "time stump" Carrying out "O.K." message (to a merchant's equipment) from a smart card. Until after a cryptographic key with this suitable is established and the information on a date and time of day is told to S, that P is checked as H suggests that it must be postponed (this is not the approach shown in drawing 3).
[0042] It returns to drawing 3 , after a Shinsei H status is generally established, S checks that the user under log in is a valid user, and a user checks that S is a just smart card. Especially the protocol of

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL FIELD

[Industrial Application] This invention relates to a smart card.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

PRIOR ART

[Description of the Prior Art] It is possible to have great count capacity in small space by progress in microelectronics. It is possible to actually put in the whole computer substantially in a credit card, and the "smart card" is created by this. Being used in order that a smart card may check the right of the card carrier which pulls down from a predetermined account typically and is carried out [for the big throughput of a smart card and memory capability] for the conventional credit card is expected. A smart card offers the guarantee of the high level of the possessor of a smart card being a just carrier. This solves the main problems of the conventional credit card. Furthermore, a smart card becomes a thing more than the "license" for pulling down from an account (an account being transferred). For example, what a smart card "carries for" the credit recognized in advance is made.
[0003] In order to enable a smart card to achieve a convention, a service provider must think it certain that the computer in a smart card cannot use it for an unjust application. In order to satisfy this need, some approaches are already used. A smart card is equipped [1st] with a power-source port and a single information passage port. The computer embedded [2nd] at the smart card operates under control of the operating system which guarantees that the instruction sent to a computer does not perform harmful actuation to the purpose and security guide of a card. That is, only the instruction which reads the permitted data area and which is ordered and changed is possible. Through remote communications, there is no publisher of today's smart card then, and he claims [3rd] using a card within the enclosure of a provider.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

EFFECT OF THE INVENTION

[Effect of the Invention] As stated above, according to this invention, the problem of security is conquered and the smart card which carried service of two or more service providers for which remote issuance is possible is realized.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention] The memory of a current smart card is sufficient magnitude to hold two or more programs and data of a service provider. That is, the memory of sufficient magnitude for visa, American Express, and a master card to live together is on a single smart card. However, in commercial semantics, the smart card which succeeded in carrying service of two or more service providers is not developed yet. It is thought that this situation is because some security issues are not solved. For example, a problem arises about what kind of authority an owner has to all the files in the memory of who is the owner of a card, and a smart card. It is the problem what authority the owner (this being also a service provider) of a smart card having in the smart card which is not in agreement with the security for which other service providers ask, speaking commercially. This is the problem of trust.
[0005] The 2nd trouble is related with remote issuance. Especially the thing for which it is required for a smart card carrier that service should be installed only by having a card at a provider's place and going is not desirable. Moreover, when one of services on a smart card is canceled, it is not desirable to require the turnover of a smart card, either. Rather, for a commercial success, it is desirable to enable remote issuance, probably it is essential, and clear.
[0006] When the trouble of remote issuance is solved, the 3rd trouble is related with the need of carrying out the reuse of the space in the smart card of a carrier, in case the old service is canceled and new service is installed.
[0007] The 4th trouble is that a provider wants so that it may restrict the commercial collision of a contention service compartment, and that a customer accesses contention service.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

MEANS

[Means for Solving the Problem] A service provider or the owner of a smart card does not have authorization in beforehand, and the above-mentioned trouble is solved by the operating system with which a service provider which is different, without accessing the file by which it was created by each existing service provider since it was each existing service provider makes it possible to live together on a smart card.
[0010] The operating system of a smart card resembles UNIX (trademark of UNIX system Laboratories) a little, it has the root directory owned by the publisher/owner of a smart card, and each service provider is a "user" installed by a publisher/owner. The subdirectory of a root directory is given to such each user, and in the subdirectory, a user creates it as a user needs a subdirectory including a file and a file.
[0011] An operating system can be made not to perform such access, when preventing from accessing the file which a user owns from other users to all the users of the smart card containing the publisher / owner of a smart card, and the carrier of a smart card is chosen. This exclusion capacity is owned by the user and other users including the publisher/owner of a smart card are realized by the password file which cannot be changed. As an option, the capacity which eliminates all the files of the given user is given to the publisher/owner of a smart card.
[0012] Moreover, an operating system has means of communications with a digital signature, and full encryption means of communications. This function gives the dependability in remote communications. By remote communications, remote issuance, effective maintenance of the database which pursues all services included in each smart card, and loss of a smart card or re-issuance of the smart card in general failure is attained.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

EXAMPLE

[Example] Some smart card operating systems are already known. One example is indicated by U.S. Pat. No. 4,816,653 (artificer: date-of-issue: [besides Anderl (Anderl)] March 28, 1989). The operating system explained below has the operating system and a well-known UNIX operating system, and many similar points. In order to help an understanding of the smart card operating system explained here, the matter of some common knowledge of a UNIX operating system is explained briefly.
[0014] A [UNIX operating system] UNIX operating system consists of a set of a file. Some of the files are called a directory file or a directory, mainly including the information about a related file. Other files are "usually" called file including user data. Moreover, in a UNIX operating system, a user can belong to specified "group (group)" which is "owner (owner)" of a file, or is recognized by the file, or can belong to "other." Each file contains a part for the data division which specifies the file descriptions, such as ownership and information accessing capability about three kinds of users. The owner of a file can change all the file descriptions.
[0015] Structurally, the first file is a root directory file. The user who is the owner of this directory is actually the owner of the whole operating system. This user can create other files to which it is pointed out by the root file. It is considered that the file is possible also for that they are also other "directory" files and being "usually" a file, and is "under" a root directory in tree top structure.
[0016] In many UNIX operating systems, one of the directories under the root is named "etc", and this directory has the file "passwd" in the bottom of it. They are "/etc/passwd" (the file "/" of the beginning of a pathname expresses the root address)., all the addresses, i.e., the pathname, of this file Generally "etc" and the "passwd" file are called the root, and are owned by the system administrator who is also an owner of a root directory. Including the encryption expression of a root password, the "passwd" file is allowed for access of the root to an operating system, only after the root logs in by showing a password. It is enciphered and the password shown is compared with the encryption password stored in the "passwd" file. When a comparison is successful, a user is accepted and access to other files is permitted to him. That is, "it means that this user had logged in."
[0017] Multiuser ability is realizable, when the root creates a subdirectory under a root directory and assigns other users the ownership of the subdirectory. Next, the root makes it possible to go into a system in the subdirectory file, when the user's password is installed in the "passwd" file and the user presents the password. Although this user has the capacity to change a self password, only by it leading the command offered by the operating system, it is possible. In a system, the password is the enciphered format and exists only in a chisel and the "passwd" file. This architecture is shown in drawing 1 .
[0018] A login process can be summarized as follows. The computer which operates under a UNIX operating system is put into operation by executing the loop formation which scans the input port of a computer. If connection by the user is detected, it will move from control to the program which started the dialogue with the user from the loop formation. The program waits a "login:" message for a response of delivery and a user to a user. Self is displayed and this makes the user identify to an operating system, when a user returns a string "htb." Next, a program must send a demand message "Password:" and a user has to present a password string. A program enciphers the password string and compares it with the

encryption password of the user in /etc / "passwd" file who identified. When in agreement, it judges that a user is Shinsei and control is passed to the file (typically, named ".profile") owned by the root. This file sets up various parameters to that user, and is passed to another file (although this is also typically named ".profile", this file exists in the directory owned by that user) owned by the user in control. After the instruction in the user's ".profile" is executed, a computer enters a loop formation and waits for the instruction of the degree from a user.

[0019] The root is the owner of all the files that constitute operating systems including the "passwd" file. Therefore, the root can change the file of arbitration, therefore is a "superuser." Even if it is the file which is not owned by the root, it is important to follow the command of the root. It is because the root has the capacity to also change the file by which the capacity of the root is controlled generally, with the "passwd" file. According to this capacity, the root has the capacity to change a password, therefore the root can always become the owner of a file. Therefore, it is meaningful to give all an owner's capacity directly to the root. If it says briefly, the root has the absolute control and all the information on all the files in a system.

[0020] (An exact password is shown) it can log in -- in addition, read-out of a file, the writing to a file, and the capacity of activation (that is, pass program control to a file) of a file are given to a user. (Nothing can be performed if there is no capacity to pass program control to the specified file.) It is because performing a program is exactly passing control to a file. Since the root can access all the files of a system, the root can read and write in and perform all files.

[0021] An instruction of all system offers of a UNIX operating system is the file which can only be performed, and these files can exist in every directory, as far as the system knows where the file is. As already stated, the root owns such all directories and files. Since the root controls read-out of all those directories and a file and authorization of activation, the root can be restricted by the user (including oneself, in being required) of arbitration by only restricting a file permission (permission) so that the file of arbitration may not be performed. Thereby, the root can create the set in which the file to which activation by a user's specific group was restricted carried out custom-made **. If it puts in another way, the root can create restricted various operating systems which contain commands fewer than all available commands by the system, i.e., "limit shell."

[0022] The absolute capacity which the root has with a [smart card operating system] UNIX operating system is unsuitable to a smart card. Although visa, the master card, and a provider like American Express probably do not permit clearly that it is the root mutually, if there is not sufficient security means clearly, it will also be thought that third persons other than these are not wanted to become the root. This is a part of trouble that a smart card does not store a commercial success which should be received.

[0023] The structure corresponding to the sensitiveness of this service provider is shown in drawing 2 . According to the structure of drawing 2 , the root owns a root directory and a number of arbitration to create of files (a directory file or regular file). For example, as for drawing 2 , there are the ".profile" file 11, the "passwd" file 12, the "log" file 17, the "filex" file 13, the "filey" file 14, and an "ID" file 18 in the bottom of it including the root directory file 10. For the bottom of the root, some subdirectories also exist and it is used as a user's (service provider) "HOME" directory, respectively. For example, drawing 2 contains the directory file 15 of the identifier (carrier of a smart card) of "htb", the directory file 20 named "bankA", and the directory file 25 named "airlineA." Each directory includes the "passwd" file (respectively 16, 21, and 26) and ".profile" file under a corresponding user's HOME directory. This is not indispensable although this arrangement of a password file has some advantages. An important thing is that the ownership of such each password file is assigned to the file and the user corresponding to the directory on [of it]. It is also useful to grant each user the ownership of directories 15, 20, and 25.

[0024] Drawing 2 includes another important directory (and user). It is the "Visitor" directory 30 and this is the entry point of the non-service provider which wants to have a dialog with a smart card.

[0025] The file architecture of drawing 2 is combined with a different operating system from a UNIX operating system. The operating system of the structure of drawing 2 mainly differs from a UNIX operating system with the operating system in that the capacity to change the file which the root does

not own is not given to the root. In order to guarantee that this function does not detour by the root, in this operating system, the root does not permit changing some files which define an operating system (in a sense, the root does not own those files). One means to realize this result is storing those non-root possession operating system files in a read-only memory (ROM). This ROM at least includes the command / module / file which performs the writing to a file. Especially the writing to a file is restricted to the thing specified by the owner of a file (the owner of a file is the user who created the file at first), and the root is only treated as other users. The command which performs the writing to a file is an operating system command like migration of a file, the copy of a file, preservation of a file, modification of a file attribute (for example, ownership), and modification of a file name. (Since it is peculiar to each smart card) Other matters installed in ROM (still more generally "1-time write-in" memory) are root run WORD and ID information on a smart card (namely, files 12 and 18). ID information can also include [that he is also only the string of arbitration, and] the identifier of a carrier. It is desirable to include the identifier of a carrier to the merchant who probably acquired ** and ID information. Each ID of root run WORD and a smart card can be stored in the file which constitutes a root directory (namely, block 10) in fact. In drawing 2 , these serve as an independent file for explanation.

[0026] In some the examples, it is the capacity for one file write-in capacity to be given to the root, and for this to delete the file of arbitration as a whole (and the file which is the process and the file deleted substantially has pointed out is deleted). A directory file and a regular file are contained in this, and it is applied also to the file which the root does not own in the file which the root owns, either. Such capacity can be given in the example to which the reuse of the room is carried out, when the given service provider does not provide the carrier of a smart card with service any longer.

[0027] Another difference between the operating system of drawing 2 and a standard UNIX operating system is a point including the code key pair by which the former was installed at the file owned by the root (for example, 13) that this key pair is peculiar to each smart card. the private key f and smart card which are secretly held by the smart card hold this pair secretly -- as -- the open key g which are not careful of is included. Of course, although both keys are known from the beginning at the owner/publisher of the smart card which is also the root user (namely, superuser) of a smart card, the root does not need to hold a private key (and destroying the information probably will be chosen). This key pair can also be included in the file which defines "an eclipse with baking", or a root directory as suitable memory like the memory containing a root password. Open key encryption is further explained to a detail later.

[0028] It is the material-difference point of a UNIX operating system and the operating system of drawing 2 to be stored in the file the password of a user's directory is owned by whose user of the. That any persons other than the owner of the file cannot read these passwords makes it possible to store in the format which does not encipher the password. It becomes impossible for the root to become the owner of the file (a regular file or directory file) of arbitration by this configuration with the limit to writing therefore, and it becomes impossible for the root to bypass the authorization set up by the owner of a file. With this material-difference point, a certain user's file becomes completely opaque to the root and other users. Thus, the configuration of drawing 2 conquers the "reliance problem" between the provider of service, and the publisher/owner of a smart card.

[0029] The following problem which should carry out [dealings security] solution is the dealings security of a smart card. This concept includes the means used by the operating system of a smart card, and those who have agreed with the communications protocol, in order to guarantee that unauthorized dealings which have a bad influence on the carrier or service provider of a smart card do not take place. This includes the activity by the root, the carrier, the service provider, the visitor (Visitor) user, or the invader. (Invaders are those who intervene in the communication link session between a smart card and the others, and replace a self message with a true message.)

[0030] One method of opposing an invader constitutes the message containing the time stump of a date and time of day, and is a thing of a message for which the part is enciphered at least. Moreover, when required, a communications protocol is possible also for requiring that a check sequence (these differs for every session) should be exchanged between persons concerned. Moreover, the effective general

approach also makes min the flow in Akifumi of delicate information like a password. These techniques are used with the below-mentioned log in and a communications protocol.
[0031] The field of [encryption] encryption is not new. The following explanation is the epitomes of two usable cipher systems only in relation to the smart card of this invention.
[0032] As everyone knows, the "secret share" method for encryption requires that two operators should share the secret function f. A way [to transmit Message m] side enciphers the message with the secret function, and forms encryption message f (m). This encryption message is transmitted and a receiving side decodes the signal received by forming Function f (f (m)). Although Function f is very difficult to discover Message m from f (m) in computational complexity, it is the function (namely, f(f (m)) =m) with which the message of a basis is restored by applying the function twice.
[0033] Although the "secret share" method for encryption is very effective, the weak spot is that there is the need (that is, it shares) of communicating a secret function. When a secret shared [the] is acquired by the wire-tapping person during a rare communication link session when the function is transmitted, it becomes already secret less.
[0034] open key encryption -- each person concerned -- a key -- an opposite -- either f or the g are held. Although one person concerned holds one key (f) secretly and does not communicate it especially, all persons are told about the key (g) of another side. therefore, the key g -- "-- it opens to the public -- having -- " -- Key f is "private." Pair f and g seem to fulfill the following three conditions.
1. g(f (m)) =m.
2. Function f cannot be determined even when g is known.
3. It is unrealizable in computational complexity to determine Message m from f (m).
[0035] Although a open key method solves the problem of the above-mentioned key distribution / management, this approach has one fault. It is slower [encryption and decode of a open key] (much computation time is needed) than a share key method.
[0036] About a smart card, transmission speed has a different significance based on the class of person concerned who is communicating with the smart card. about the publisher / owner, and the service provider of a smart card, a rare thing expects a communication link -- having -- therefore, the processing time -- "-- since it is not maximum important", low speeds are not main faults. However, in the communication link with the other person (namely, merchant who logs in as a visitor user), the rate is important.
[0037] The problem of a rate will be solved by combining a "share secret" method with a open key method, if required. That is, when starting a communication link, temporary "share secret" is communicated between a smart card and a merchant using a open key method. Especially the side that has a open key presents a "share secret", and communicates it to the side which has a private key. Then, all messages are enciphered more at a high speed using a "share secret" method.
[0038] Or it is also possible to use an authentication (using share secret) method. By the authentication method, a message is transmitted by Akifumi and a "digital signature" is added (that is, "signed"). A "digital signature" is the hashing (for example, a certain number addition of the ASCII code of the alphabetic character in a message as law) of the message encoded. Of course, with application it is guaranteed to be that an invader cannot replace true data by fake data, information can be sent by Akifumi (after the validation process which probably used ** and a open key).
[0039] Use of a open key method solves almost all the problems of key management. Although the problem of the initial information on the open key of the person concerned who wants to communicate with a smart card remains in addition, since the smart card itself can offer the information, it is not a problem.
[0040] Since [install of log in [by the root], and service provider/user] encryption guarantees a safe communication link, the publisher/owner of a smart card can trust remote install of service. Of course, a publisher/owner (namely, root) has to log in to a smart card first. The protocol for a log in is shown in drawing 3 . Moreover, the protocol for a service installation process is shown in drawing 4 . Connection of RIMOTO is shown to a possible physical target between the smart cards of this invention at drawing 8 .

[0041] As shown in drawing 3 , a process is started from the possessor (P) of a smart card being attested as a Shinsei smart card (S) carrier. As shown in drawing 3 , a process is started by inputting a possessor's PIN (personal identification number) into a smart card as the prompt from a smart card. It is advantageous to the equipment which may catch PIN to use the throughput of a smart card, in order to attest a possessor at the point that it is not necessary to communicate an PIN string. Even if it is the application with which P and S exist within the enclosure of a merchant, a merchant's equipment can be considered as the equipment of the stand-alone mold which carries out an interface to a smart card at insurance. This equipment can check operating by the cell, having a keyboard and a display, and not having other ports, processors, and memory that can be written in. At the time of actuation, P inserts S in this stand-alone equipment, PIN is inputted by the keyboard, and, as for a smart card, that PIN judges whether it is the right. If right, the display of the equipment will output a message "O.K." When such stand-alone equipment is not available (in the remote ****** case [A communication link like / when using a "dam" card reader at a possessor's home / Or for example,]), PIN shown should be processed within the smart card and it is enciphered by "time stump" Carrying out "O.K." message (to a merchant's equipment) from a smart card. Until after a cryptographic key with this suitable is established and the information on a date and time of day is told to S, that P is checked as H suggests that it must be postponed (this is not the approach shown in drawing 3).
[0042] It returns to drawing 3 , after a Shinsei H status is generally established, S checks that the user under log in is a valid user, and a user checks that S is a just smart card. Especially the protocol of drawing 3 advances as follows as a whole.
[0043] a. Urging an input to S, P presents an PIN string. Within a smart card, PIN exists in the file (for example, file 14 of drawing 2) of the root possession opened in order that a carrier might change. If S is in agreement as compared with the PIN string in whom the shown PIN string is stored, it will mean that P was checked as H.
[0044] b. Cautions can be turned to the communication link between S and O if H is checked. S displays self by showing O the ID number and the password challenge RND1 in a random string's format.
[0045] c. O enciphers RND1 with the password of O, forms a string K1 (RND1), and returns it to S. The format of this password response changes for every session clearly, and it guarantees that the true password of O is not stolen by the invader. The password of all smart cards which O owns was held where, and the problem which such a database says how much whether is insurance remains. However, O does not need to hold the database of a password in fact. When the thing which is the need is processed with the data supplied by S to O, he is only the single seed who becomes the password of a smart card. The data is ID information.
[0046] d. In order to guarantee that he is not playback of record of an initial string (ID, RND1) since the string presented by the smart card is always the same or strange in advance to O, it may ask for an additional authentication step. This is realized when O sends to S the challenge message RND2 which consists of the ID and random string.
[0047] e. Based on ID contained in RND2 string, S judges with O being a user, acquires a required key (for example, password of O), and decodes K1 (RND1). When it comes to RND1, S judges with O being Shinsei as a result of decode.
[0048] f. After that, S enciphers a string RND2 by the root run WORD of S, and transmits the string K1 (RND2) of the result to O.
[0049] g. O decodesK1 (RND2) response, and when the string of the result is RND2, it is satisfied with S being just of O. End a login process now, and O shows S a prompt and will be ready for receiving the demand of service of O.
[0050] The above-mentioned "log in" process may notice it seeming to differ from the login process of common knowledge which a computer to access controls. A computer requires a user's initial identification information and then requires a password. Based on the initial identification information, a computer gets to know which password is expected. On the other hand, a smart card seems to be controlled by semantics of starting a communication link (O). However, a smart card offers information, ID and RND1, instead of requiring initial identification information (information being acquired).

[i.e.,] This causes the problem whether the response from O is initial identification information, and whether to be it and a password. If this is a password, how does the password get to know whether it is the right, as for S? I hear that the response from O is used for three purposes, and the answer has it. In order to display self in the sense of initial identification information and to encipher RND1 (ID contained in RND1), by using a right key, O attests self and asks the justification of S by RND2 returned in encryption mode.

[0051] If it logs in to O, H can communicate the demand of install of the service offered by the service provider (SP). Although the communication link about the specific service required as being installed by O may include a dialogue with human being, it is also automatable. For example, the service for which it asks is communicated to S, and H can be communicated with O by S. The protocol for install of service to drawing 4 is shown.

[0052] a. H transmits a service request to S.

[0053] b. S enciphers this demand and transmits it to O. The electronic communication link between O and S can be enciphered with the private key element of the open key in S. S sends the open key to O. Or a communication link can be enciphered also in "share secret" of a smart card. It is possible to offer temporary "share secret" from O (using open key encryption as mentioned above) to S possible [choosing root run WORD as a "share secret"]. In drawing 4 , root run WORD is used for encryption and the demand string K1 (REQ) is created.

[0054] c. If the demanded service is got to know, O will communicate with SP and it will check agreeing that SP provides H with service.

[0055] d. -- if it agrees with SP on offer of service, after O chooses a temporary password and notifies the password by ******** communication link probably -- at SP, it will create the directory and password file for SP in S.

[0056] e. if a password file is set up for SP user, that temporary password will be sent to S by encryption communication link above, and the ownership of this directory and a password file will be transferred to SP (this password is available as a "share secret" key in a communication link session with future SP). Moreover, the other application software which SP needs can be installed at this time, and O transmits those files in encryption mode. Or application software can be set up also so that it may not be installed by O.

[0057] f. It is notified to H that it communicates with SP for the last setup at this time.

[0058] g. H uses a login sequence like drawing 3 , however uses a temporary SP password as a cryptographic key, and sets up the channel between S and SP.

[0059] h. If a log in in SP is established, S sends out a service request, and SP will answer and will install a new password, the required file which was not installed by O, and data. A service installation process is completed now.

[0060] [offer of service by the service provider] -- as mentioned above, a service provider is a user who only has the directory assigned to the smart card. A service provider logs in, if a processor establishes the communication link between a smart card and a service provider. There are three elements in a log in protocol like [front].

(1) SP wants to decide that P is H.

(2) I want to judge that S is SP of truth [user / who logs in].

(3) SP wants to judge communicating with just S.

[0061] These three elements are performed with the protocol explaining drawing 3 . A service request can be advanced only after a log in success. A service request is requiring that H should install "money" in SP (for example, bank) by filling the "smart card" of S at S. Restoration of a smart card is installing the value which is only in a certain file owned by SP, for example. This is shown in the flow chart of drawing 5 .

[0062] [a dialogue with a merchant] -- when generous enough, thinking that a smart card carrier wants a smart card and the merchant who is a visitor (V) user to have a dialog is expected. According to the above-mentioned method, such a dialogue is possible by two approaches. One is the direct dialogue of a smart card and a merchant, and another is a dialogue between 3 persons containing a smart card, a

merchant, and a service provider. The protocol for the interactive mode between 3 persons is as being shown in drawing 6 , and is as follows.
[0063] a. P establishes a communication link between S and V (remote connection of the S is carried out [passing S to V or] to V).
[0064] b. Urging an input to S, P presents an PIN string. If this is surely in agreement, S will judge with P being H, will progress to a standard "log in" sequence, and will send the ID information and RND1.
[0065] c. V sets up a channel with SP, displays self on SP, and relays ID information and RND1.
[0066] d. If ID information is given, SP will determine the password (a seed string also using it with ** and processing probably), and will encipher RND1 with the password. The string K2 (RND1) of the result is seen off in S with the random string RND2.
[0067] e. S judges whether the right password was used, in case SP forms K2 (RND1), if the conclusion is truth, will encipher RND2 and, as a result, will transmit K2 (RND2) to SP.
[0068] f. SP will notify that a prompt can be progressed to the demand of use at V of S to delivery and a merchant, if it checks that S has enciphered RND2 using a right password.
[0069] g. V requires action (for example, or it deletes a certain value from the account of H which SP has, a value with the file which is in S and is owned by SP is changed) from SP.
[0070] h. SP fills the demand, and if required, he will send the suitable command enciphered with SP password to S.
[0071] Those who do not have the relation established a smart card and beforehand need to establish the mechanism which makes it possible to log in to a smart card to a smart card to converse with a merchant (or merchant who tied up with a merchant's bank or those who provides a merchant with service and does instead of [of a merchant]) directly. A "visitor" user directory fills this demand and this user does not have a password. Since a visitor user is a user who does not have security very much as a result, access of V must be controlled strictly.
[0072] for example, such a visitor user can access one problem with the need of solving at the application file (program) of only the service provider specified by the merchant -- or it is whether to be able to access the application file of all service providers. When access to the application file of all service providers is permitted, the easiest method is that the root sets up a visitor user directory without a password, and a visitor user gives the limit shell which makes it possible to perform only the set with which the operating system command was restricted. That is, it sets up so that one directory (only some operating system commands are included) owned by the root in Variable PATH and SP subdirectory (or subdirectory which the service provider/user chose) containing the executable file with which SP wants to permit a visitor user execute access may be included.
[0073] When permitting access to the application file of only SP who specified, of course, SP must be specified and the means only containing the executable file of SP who specified must be established. Also in this case, this is easily realized by limit shell, and a PATH variable includes SP's specified directory (or selected subdirectory). A protocol is as being shown in drawing 7 , and is as follows.
[0074] a. Urging an input to S, P presents an PIN string. If this is surely in agreement, S will judge with P being H, will progress to a standard "log in" sequence, and will send the ID information and RND1.
[0075] b. Since V does not have a password, it only returns a string RND1.
[0076] c. By this response, S recognizes that a user is a visitor user and sends out the open key Kpu. (The open key can also already be sent as a part of ID information) At this time, S can also send the "digital signature" drawn from the message containing a open key, ID information, and RND1. Moreover, S can also see off the encryption string who constitutes the "share secret" (not shown to drawing 7) to propose. A digital signature is enciphered by the open key.
[0077] d. V decodes a "digital signature" using the offered open key. When the decoded "digital signature" is in agreement with a suitable string, V sends out RND2.
[0078] e. S enciphers RND2 by the open key, and answers by Kpr (RND2).
[0079] f. V decides communicating with S, when this message is decoded by Kpu and RND2 is acquired.
[0080] g. V enciphers the information on time of day and a date by Kpu, and delivery and S return a

prompt to S.
[0081] h. Similarly encipher by Kpu, V transmits a demand (action for which V asks, and SP used are identified) to S, and S answers by authorization which communicates with specified SP. This authorization is enciphered by the open key Kpr.
[0082] Generally, a merchant thinks that he wants to obtain the fund belonging to H in exchange for the goods or service offered by the merchant. As mentioned above, a service provider like a bank is completely able to install the "smart card" holding a certain value. This value exists in a certain file owned by the service provider.
[0083] Although it thinks that a merchant wants to access this file and SP (it has tied up with H) permits access to this file, that authorization is made, only by being restricted very much and controlled strictly. Thus, SP is the identifier of the convention expected by the operating system, he creates a certain file, puts a certain value and a specific operating system command (this is not owned by the root) into the file, accesses the file, and deducts the amount of money from the value in the file.
[0084] Such a command-stream Fig. is shown in drawing 9 . With block 200, a command is started by referring to the file (specified identifier) in a visitor user directory. This file must contain four entries divided by the line-feed character, and it is assumed that an operating system consists of the amount of money which this four entry c Deducts with a date and time of day, and b merchant's ID (for example, an identifier, the address, and probably ** code), and a service provider which has the "smart card" of which d use is done.
[0086] When this file does not exist, or when it does not have a demanded number of entries, it moves to block 210 and control notifies a merchant (visitor user) of this lack. When a file exists, a command reads the value in the "smart card" file of a service provider (SP) with block 220. It evaluates whether block 230 has the amount of money larger than the value in a smart card which a merchant wants to pull out. When the amount of money is larger, it moves to block 240, and control constitutes a refusal message, and transmits it to a merchant and the log file in a smart card. When the amount of money is lower than a value, it moves to block 250, control is a log file, and it inspects whether there are any various unjust signs. This can also be considered as another command called by the command under activation. As shown in drawing 3 , block 250 may produce three kinds of outputs. The 1st suggests potential unjust conditions (for example, this merchant used more smart cards than a regular count in the time interval chosen in advance). The 2nd answers the threshold file which it is provided by SP and a merchant is made to discuss with SP about dealings. The 3rd displays reference condition.
[0087] Potential unjust conditions are processed using the information stored in the log file of a carrier (block 260), and it moves from control to block 240 after that. The information stored identifies a merchant, the frame which it was going to pull out, the reason for refusal, etc. This provides a carrier with information required to converse [the publisher / owner of a card, and] with government authorities, if required. If needed, when there is misgiving of unjust conditions, a smart card is made into an invalid.
[0088] When the threshold set up by SP is exceeded ("real time" for example, SP asked for the drawer authorization exceeding 1000 dols), a message consists of blocks 270 and it moves from control to block 280.
[0089] Block 280 reaches directly from block 250, also when standard condition is shown. Block 280 increments the sequence number in the log file of a smart card, and deducts the amount of money which a merchant demands from the amount of money in a value file. Then, block 290 creates a new sequence number, a date and time of day, a merchant's identification information, the amount of money, and the string that consists of an SP. Block 300 creates a string's digital signature and block 310 creates the message which consists of the message which consisted of blocks 220, a string who consisted of blocks 300, and a digital signature. Finally, this message is sent to a merchant and the log file of a smart card.
[0090] A merchant's equipment performs one of two things. When the message discussed with SP exists, a merchant's equipment is connected to SP and the message created with block 310 is transmitted. Then, a merchant can get a credit the instancy to the amount of money (as long as it is concluded, of course based on a signature that the message is just). When the message received by the merchant does not

contain the message constituted by block 220, only a merchant stores an authorization string, collects such authorization strings covering the selected time interval (for example, employment day whole), and transmits the authorization string to suitable SP after that.
[0091] Although the authorization string is shown are enciphered by the open key of S, enciphering with SP's specified password is also possible. An authorization string must be firm enough so that it may guarantee that a merchant only does count reproduction of predetermined of it, and does not send to SP. This is realizable by some approaches. Having the display of the value of "before" and the "back", having the sequence number supplied by S, etc. are included in it. [in having the time stump of a date and time of day and a value file] That this authorization string cannot decode [therefore] by V, since modification is impossible, security is held.
[0092] One description of the smart card publisher as a service center / [owner] this invention is having the general knowledge of a service provider the publisher/owner of a smart card (O) having the "application" which exists on a smart card, and controlling the service provider. O controls [1st] a setup of the directory of a service provider. O can delete [2nd] the directory of arbitration (not concerned with the existence of the consent of a carrier), when O can access a smart card, corresponding to the demand of a carrier. The 3rd O is the identification information of all the service providers that share a smart card, and the only person concerned who gets to know various details of those service providers. O can control [4th] the number of the service providers the amount of the memory which can access each service provider is controlled, therefore "can be lived together" on a smart card through the design of an operating system. O can define [5th] the grouping of a service provider to dealings of specific classes. O can charge [6th] such each service provider in proportion to the space occupied by the service provider to the right which exists on a smart card.
[0093] Some profits arise from the method of this invention so that clearly from all the above-mentioned things. Having not stated above "fixes" a card with a defect, and O has the capacity which re-installs all services (an owner's typical capacity). On the contrary, O has the capacity to delete all directories, and this capacity is executed when judged with the violation of security having occurred.
[0094] About security, there is an attack of four formats with the need of taking into consideration. The 1st is the case where an invader is going to become the root. The 2nd is the case where an invader is going to turn into a service provider. The 3rd is the case where a person concerned (the root, a service provider, an invader, a visitor, carrier) is going to do the thing except the permission being granted. The 4th is the case where a possessor is not a carrier of Shinsei.
[0095] About the attack of the 1st format, the first main gateway is root run WORD. This is an effective gateway in the semantics of being set up so that an operating system may make a smart card an invalid completely, when it fails, although the log in as the root was tried. For example, all directories are eliminable.
[0096] Trying to log in as a service provider should be treated only by the slightly loose approach. That is, it is possible to set up so that a counter may pursue the trial to which it was going to log in as a service provider and which went wrong. A smart card becomes an invalid when the count of trial failure exceeds the value (for example, 4) chosen in advance. It is also possible to also use the invalid of a smart card only as the directory of the service provider which was an offensive object in such a situation, and to make it all service provider directories other than a root directory.
[0097] As mentioned above, much communications are things with a smart card to depend on a visitor user most. It needs to be careful although it is necessary to make these communications flexible. Although a kind message comes out in a UNIX operating system to executing the command which is not in PATH, a smart card needs to supervise these trial that is going to access the command which is not allowed. A counter is used also in this case, when the count chosen in advance is exceeded, the communication link with a visitor can be ended, a message can be stored in a smart card, and a card can be made into an invalid to persons other than a carrier. The message which will be stored in the directory of a carrier consists of a detail of the interrupted dealings. Although the same action occurs also when a carrier tends to execute an unauthorized command, a diagnostic message is written in a root possession file in that case.

[0098] Another security means may be related also to the just dealings by the visitor. As mentioned above, a log file is in one of the files owned by the root, and this holds record of all dealings performed by the smart card. When the given time interval has too much many dealings by one visitor and specific situations when the given time interval has too much many dealings exist, this file can be checked so that no specific visitor user or specific visitor users may be permitted.
[0099] Although the person concerned who communicates with a smart card is O.K., when the possessor of a card has a problem, a slightly different security issue arises. In this case, henceforth [it] at that time, the person concerned who is having a dialog with the smart card is easily assumed to think that he wants to cooperate in preventing use of a smart card. This is realized by some approaches. For example, when ID presented by the possessor into the login sequence is an error (for example, since a smart card is stolen), a merchant can execute the command which writes a message in the file belonging to the root, and can make a card an invalid. In this case, the only approach of restoring a card is communicating with the root. When the root reads the diagnostic message in the file, a possessor can judge in practice whether it is a true carrier, and can take suitable action.
[0100] If the above-mentioned structure and the above-mentioned operating system of a smart card are given, it is clear that the publisher/owner who installs all services on a smart card have the knowledge of those services. That is, although a publisher/owner does not have the capacity to investigate the inside of the file owned by various (he is the root owner of a smart card) service providers, the publisher/owner knows about which service provider exists on each smart card. This knowledge can be held in the database owned by a publisher (each smart card can also hold such information about itself)/owner.
[0102] When a smart card is lost or it damages, the new smart card which installed all the service providers from the beginning can be published to a carrier. The unrecoverable only items are the data file created by various users in the old file, and the password of a service provider. About initial install, the set of a temporary password file is installable. Then, a publisher/owner communicates with a service provider, and it notifies about a temporary password, and a carrier can communicate with a service provider, can change the password, and can put in a file required for each directory.
[0103] [Audit trail] As mentioned above, the root holds a log file and stores record of each dealings in it. Then, this file can be used in order to pursue various thresholds to impose a carrier or a service provider.

[0104] Too much use of a smart card has the possibility of a display of an unauthorized use. As mentioned above, the careful monitor of a log file can detect such use, and it is suspended by it.
[0105] However, the thing about completely just use is also possible as another usage of a log file. For example, carrying out "batch" transmission from a merchant to all small dealings, (at end which is probably ********) when a credit offer service provider receives the burden exceeding a certain limitation, I can have it notified on "real time." About the smart card of a smart card, a carrier can communicate with the bank of a carrier automatically, when less than a limitation with the amount-of-money value in a smart card, and it can be ordered to change an additional fund to a smart card further.
[0106] Another usage is the thing about dispute settlement of an audit trail further. When a merchant insists that he was used in order to acquire goods or service with a smart card and a carrier fights for the opinion, a log file can be used in order to solve the dispute.
[0107] A [cooperation between service providers] service provider is completely able to carry out a cooperative tie-up. Such a tie-up can specify various activities performed by the smart card, when a smart card is accessed and when or a smart card is accessed by the specific user. The number of such possibility is unrestricted and the following examples are the things for mere instantiation.
[0108] For example, Firm Z presupposes that the missionary salesman who needs to purchase a gasoline probably quite periodically is employed. O is required for Z to communicate with O, to make each salesman (carrier) publish a smart card, and to install G as a gasoline provider by making Z into a service provider. Z contracts a contract with behind as a provider of a credit to Bank B and a salesman for a while. This service can be installed in all the smart cards belonging to a salesman by RIMOTO by obtaining cooperation of G.
[0109] A smart card has a dialog with G, and especially Z can require G to install so that the

communication link with O may be required, when it discovers that B is not a user, although Z is a user. There being the need that G carries out is sending a suitable command, when a right smart card logs in by G.

[0110] Although the above-mentioned explanation described the "smart card", this invention considers in fact the individual humanity news equipment of the arbitration which meant moving to the place to which people go in connection with the man anywhere fundamentally. That is, as an intention of a claim, the vocabulary a "smart card" is designed a sake [for individual treatment], and includes at least all the equipments that meant that some of the function carried the information about an individual. This contains a cellular phone machine and a personal communicator clearly. These have an electronic means (for example, processor) required to already make it possible to carry out this invention, and current expectation is that they come to carry these electronic instruments as people usually carry a credit card.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is drawing of the structure of a UNIX operating system.
[Drawing 2] It is drawing of the tree structure of a smart card operating system.
[Drawing 3] It is drawing of the log in protocol between a smart card, and its publisher/owner.
[Drawing 4] It is drawing of the protocol in connection with a smart card, its publisher / owner, and a service provider.
[Drawing 5] A smart card is drawing of the protocol which acquires service from a service provider.
[Drawing 6] It is drawing of the protocol in connection with a smart card, a visitor user, and a service provider.
[Drawing 7] It is drawing of the protocol between smart cards and visitor users without connection with a service provider.
[Drawing 8] It is drawing of the arrangement which carries out remote issuance of the smart card using a telecommunication network.
[Drawing 9] It is the flow chart of the operating system command which pulls out the value memorized by the file of a service provider.

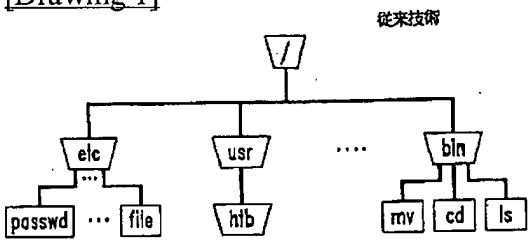
[Translation done.]

* NOTICES *

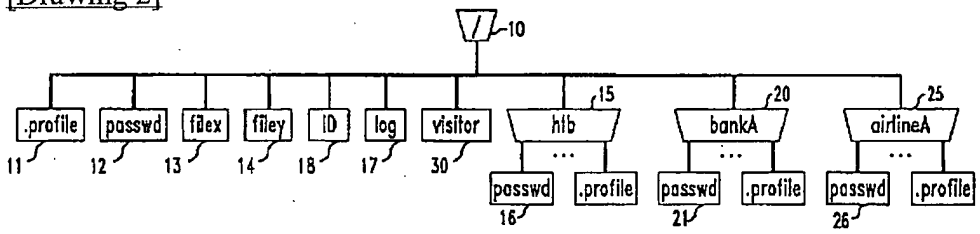
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

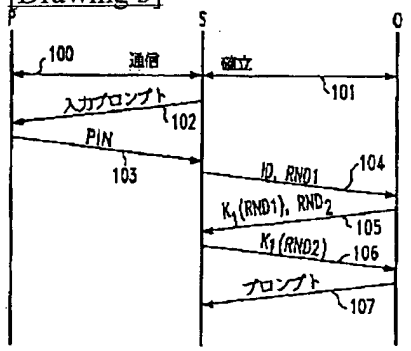
[Drawing 1]



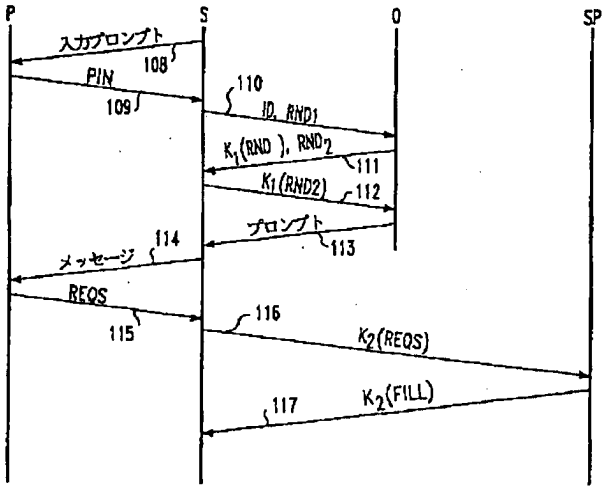
[Drawing 2]



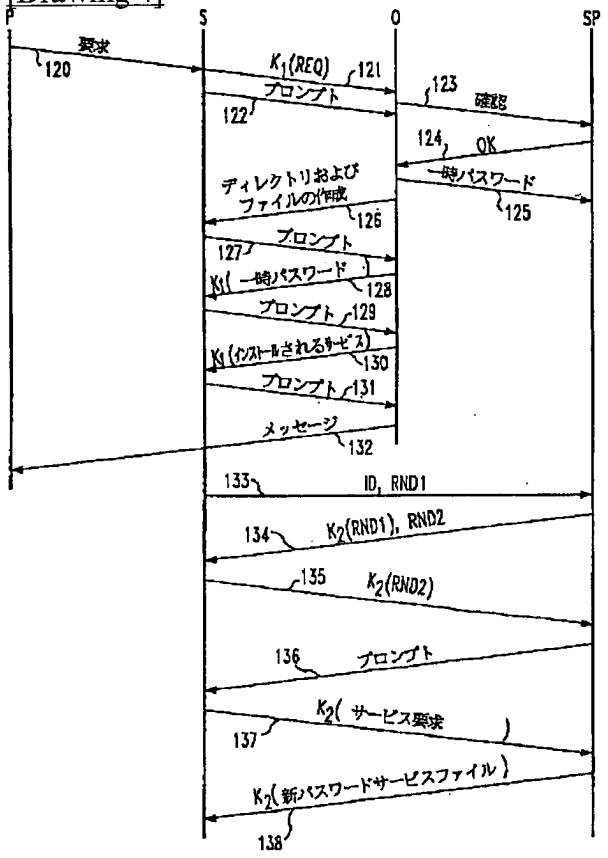
[Drawing 3]



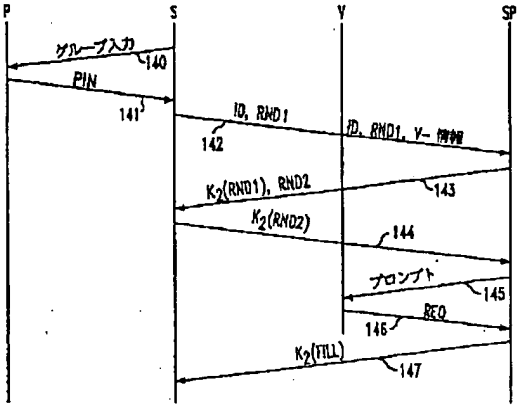
[Drawing 5]



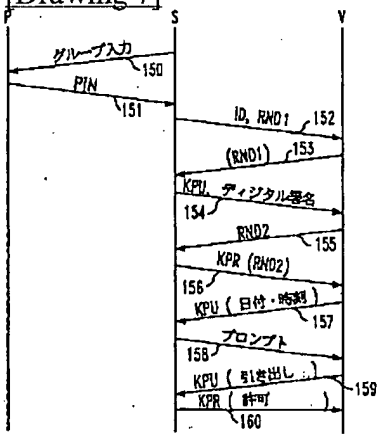
[Drawing 4]



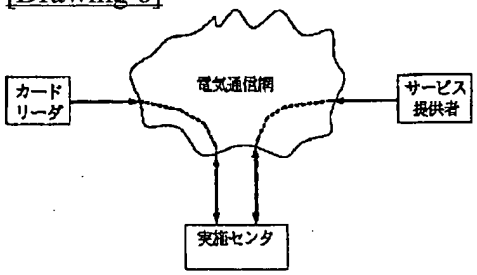
[Drawing 6]



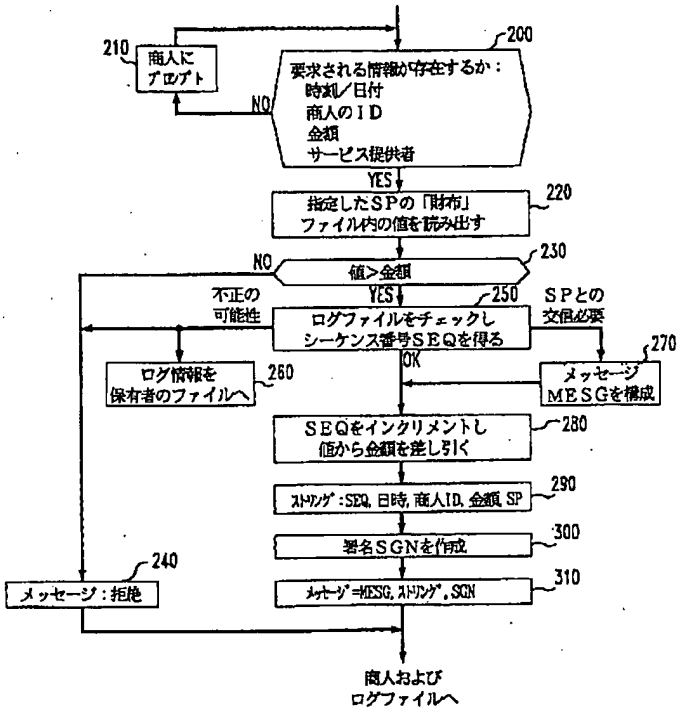
[Drawing 7]



[Drawing 8]



[Drawing 9]



[Translation done.]